Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* ○ *The USB stick contains personal photos of Jorge's family and pets, along with work-related documents such as a new hire letter and employee shift schedules.* ● *Are there sensitive work files?* ○ *These files include both personal and company-sensitive information.* ● *Is it safe to store personal files with work files?* ○ *It is not safe to store personal files with work files, as personal data could be used to target or manipulate the individual.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees?* ○ *An attacker could use the new hire documents to impersonate an employee and damage the HR department's reputation or gain unauthorized access to internal systems.* ● *Could the information be used against relatives?* ○ *Information about Jordan's upcoming wedding could be exploited to target relatives with scams, such as pretending to be Jordan in need of urgent financial help.* ● *Could the information provide access to the business?* ○ *The attacker could use Jorge's name and documents to create a fake identity, access internal hospital files, or distribute malware through compromised credentials.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* ○ *If the device contained malware such as a Trojan horse, ransomware, or fileless malware, it could compromise the system as soon as it is plugged*

	in. These threats might operate silently in the background, collecting credentials or spreading through the internal network. ● *What sensitive information could a threat actor find on a device like this?* ○ *Sensitive data—such as patient records, employee details, or onboarding documents—could be harvested and exploited.* ● *How might that information be used against an individual or an organization?* ○ *A threat actor could use this information to demand ransom from the hospital in exchange for not leaking the data, or impersonate staff members to gain deeper access to critical systems.* ○ *To prevent such attacks, organizations should enforce strict USB policies, use endpoint protection with auto-scan capabilities, and train employees not to connect unknown devices to company systems.*